PENDING CLAIMS AS AMENDED

Please amend the claims as follows:

1. (Previously Presented) A method for configuration management for a computing device, comprising:

providing available software to be loaded into said computing device to update a resident software within said computing device;

determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

updating said resident software with said available software if said resident software and said available software are not authenticated;

setting an authentication flag if said resident software is not authenticated but said available software is authenticated; and

updating said resident software if said resident software is not authenticated but said available software is authenticated.

2. (Currently Amended) A method for configuration management for a computing device, comprising:

providing available software to be loaded into said computing device to update a resident software within said computing device;

determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

rejecting said available software if said resident software is authenticated and said available software is not authenticated; and

updating said resident software with said available software if ~~one of the following three conditions is met:~~

~~(1) said resident software and said available software are authenticated,~~

~~(2)~~ said resident software and said available software are not authenticated~~;~~

~~(3) said resident software is not authenticated but said available software is authenticated~~.

3. (Previously Presented) The method of claim 2 wherein said determining whether or not said resident software is authenticated comprises of:

determining whether or not an authentication flag has been set;

wherein said resident software is determined to be authenticated if an authentication flag has been set; otherwise

said resident software is determined to be unauthenticated.

4. (Previously Presented) The method of claim 3 wherein said authentication flag is set when said authenticated software is loaded onto said computing device if said resident software is not authenticated but said available software is authenticated.

5. (Previously Presented) The method of claim 4 wherein said authentication flag is set by a service technician.

6. (Previously Presented) The method of claim 2 wherein said determining whether or not said resident software is authenticated comprises of performing a direct authentication procedure on said resident software.

7. (Previously Presented) The method of claim 6 wherein said performing a direct authentication procedure comprises performing a cyclic redundancy check.

8. (Previously Presented) The method of claim 6 wherein said performing a direct authentication procedure comprises performing a secure hashing algorithm.

9 - 20. (Canceled).

21. (Previously Presented) An apparatus for configuration management for a computing device, comprising:

means for providing available software to be loaded into said computing device to update a resident software within said computing device;

means for determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

means for determining whether or not said available software is authenticated;

means for updating said resident software with said available software if said resident software and said available software are not authenticated;

means for setting an authentication flag if said resident software is not authenticated but said available software is authenticated; and

means for updating said resident software if said resident software is not authenticated but said available software is authenticated.

22. (Currently Amended) An apparatus for configuration management for a computing device, comprising:

means for providing available software to be loaded into said computing device to update a resident software within said computing device;

means for determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

means for determining whether or not said available software is authenticated;

means for rejecting said available software if said resident software is authenticated and said available software is not authenticated; and

means for updating said resident software with said available software if ~~one of the following three conditions is met:~~

~~(1) said resident software and said available software are authenticated,~~

~~(2)~~ said resident software and said available software are not authenticated~~,~~

~~(3) said resident software is not authenticated but said available software is authenticated~~.

23. (Previously Presented) A computer-readable medium embodying instructions, which when executed by a processor, implement a method for configuration management for a computing device, the method comprising:

providing available software to be loaded into said computing device to update a resident software within said computing device;

determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

updating said resident software with said available software if said resident software and said available software are not authenticated;

setting an authentication flag if said resident software is not authenticated but said available software is authenticated; and

updating said resident software if said resident software is not authenticated but said available software is authenticated.

24. (Currently Amended) A computer-readable medium embodying instructions, which when executed by a processor, implement a method for configuration management for a computing device, the method comprising:

providing available software to be loaded into said computing device to update a resident software within said computing device;

determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

rejecting said available software if said resident software is authenticated and said available software is not authenticated; and

updating said resident software with said available software if ~~one of the following three conditions is met:~~

~~(1) said resident software and said available software are authenticated,~~

~~(2)~~ said resident software and said available software are not authenticated~~,~~

~~(3) said resident software is not authenticated but said available software is authenticated~~.

25. (New) The computer-readable medium of claim 24, wherein the method further comprises:

determining whether or not an authentication flag has been set;

wherein said resident software is determined to be authenticated if an authentication flag has been set; otherwise

said resident software is determined to be unauthenticated.

26. (New) The computer-readable medium of claim 25, wherein said authentication flag is set when said authenticated software is loaded onto said computing device if said resident software is not authenticated but said available software is authenticated.

27. (New) The computer-readable medium of claim 26, wherein said authentication flag is set by a service technician.

28. (New) The computer-readable medium of claim 24, wherein said determining whether or not said resident software is authenticated comprises of performing a direct authentication procedure on said resident software.

29. (New) The computer-readable medium of claim 28, wherein said performing a direct authentication procedure comprises performing a cyclic redundancy check.

30. (New) The computer-readable medium of claim 28, wherein said performing a direct authentication procedure comprises performing a secure hashing algorithm.

31. (New) The apparatus of claim 22, wherein said means for determining whether or not said resident software is authenticated comprises:

means for determining whether or not an authentication flag has been set;

wherein said resident software is determined to be authenticated if an authentication flag has been set; otherwise

said resident software is determined to be unauthenticated.

32. (New) The apparatus of claim 31, wherein said authentication flag is set when said authenticated software is loaded onto said computing device if said resident software is not authenticated but said available software is authenticated.

33. (New) The apparatus of claim 32, wherein said authentication flag is set by a service technician.

34. (New) The apparatus of claim 22, wherein said means for determining whether or not said resident software is authenticated comprises means for performing a direct authentication procedure on said resident software.

35. (New) The apparatus of claim 34, wherein said means for performing a direct authentication procedure comprises means for performing a cyclic redundancy check.

36. (New) The apparatus of claim 34, wherein said means for performing a direct authentication procedure comprises means for performing a secure hashing algorithm.

37. (New) Apparatus for configuration management for a computing device, comprising:

a processor configured to:

provide available software to be loaded into said computing device to update a resident software within said computing device;

determine whether or not said resident software stored in a storage device associated with said computing device is authenticated;

determine whether or not said available software is authenticated;

reject said available software if said resident software is authenticated and said available software is not authenticated; and

update said resident software with said available software if said resident software and said available software are not authenticated, and

a memory coupled to the processor for storing data.

38. (New) The apparatus of claim 37, wherein said determining whether or not said resident software is authenticated comprises:

determining whether or not an authentication flag has been set;

wherein said resident software is determined to be authenticated if an authentication flag has been set; otherwise

said resident software is determined to be unauthenticated.

39. (New) The apparatus of claim 38, wherein said authentication flag is set when said authenticated software is loaded onto said computing device if said resident software is not authenticated but said available software is authenticated.

40. (New) The apparatus of claim 39, wherein said authentication flag is set by a service technician.

41. (New) The apparatus of claim 37, wherein said determining whether or not said resident software is authenticated comprises performing a direct authentication procedure on said resident software.

42. (New) The apparatus of claim 41, wherein said performing a direct authentication procedure comprises performing a cyclic redundancy check.

43. (New) The apparatus of claim 41, wherein said performing a direct authentication procedure comprises performing a secure hashing algorithm.

44. (New) An apparatus for configuration management for a computing device, comprising:

a processor configured to:

provide available software to be loaded into said computing device to update a resident software within said computing device;

determine whether or not said resident software stored in a storage device associated with said computing device is authenticated;

determine whether or not said available software is authenticated;

update said resident software with said available software if said resident software and said available software are not authenticated;

set an authentication flag if said resident software is not authenticated but said available software is authenticated; and

update said resident software if said resident software is not authenticated but said available software is authenticated, and

a memory coupled to the processor for storing data.

45. (New) The apparatus of claim 44, wherein said authentication flag indicates whether authenticated software is loaded into said computing device.

46. (New) The method of claim 1, wherein said authentication flag indicates whether authenticated software is loaded into said computing device.

47. (New) The apparatus of claim 21, wherein said authentication flag indicates whether authenticated software is loaded into said computing device.

48. (New) The computer readable medium of claim 23, wherein said authentication flag indicates whether authenticated software is loaded into said computing device.